Updated 05/13/2025

Sign up

Blue Team Level 1 certification training

All-In-One: Preparation & Exam included in the price

2 days (14 hours)

Presentation

Our Blue Team Certification 1 course will enable you to validate your practical and technical skills in defensive security and make your entry into the world of cybersecurity. Blue Team Level 1 (BTL1) is the 100% hands-on "junior" certification issued by the British organization Security Blue Team.

Our training program targets profiles with 0 to 2 years' experience who want to demonstrate their defensive skills in a Level 1 SOC environment.

On completion of this course, you will be able to identify, exploit and document vulnerabilities, and propose solutions to strengthen and optimize an organization's IT security.

Objectives

- Master the 5 main defensive areas assessed by BTL1 (phishing, TI, DFIR, SIEM, IR)
- Produce clear, usable reports for security teams
- Pass the BTL1 exam

Target audience

- Junior or aspiring SOC analysts
- Anyone wishing to take their first steps in cybersecurity

Prerequisites

- There are no prerequisites to follow the training course, which will prepare you to sit the exam.

Blue Team Level 1 Certification Training Program

Fundamentals & Life of a SOC

- blue-team roles: N1 / N2 analyst, junior threat intel, junior forensic scientist
- OSI models, network devices & basic segmentation
- Workstation/server security: hardening, anti-malware, logging
- SOC soft-skills: stress management, alert prioritization
- BTL1 course presentation: 330 lessons, 23 labs, 4-month access

Phishing Analysis & Email Threats

- Attack types: BEC, drive-by, vishing, credential-harvesting
- Artifact collection: headers, attachments, web sandboxes
- IOC tools: VirusTotal, URLscan, CyberChef, PhishTool
- Countermeasures: SPF, DKIM, DMARC & response playbooks
- Writing a BTL1-compliant phishing incident report

Digital Forensics & Threat Intelligence

- Windows artifacts: EVTX, Registry, JumpLists, $MFT
- Memory & disk analysis: Volatility, Autopsy, FTK
- PCAP & C2 detection: Wireshark, Suricata rules
- Watch models: strategic, operational, tactical
- MISP / OpenCTI platforms: ingestion, enrichment, IoC distribution

SIEM, Detection & Monitoring

- Splunk: stats queries, transactions, SOC dashboards
- ELK & Sigma: cross-log correlation, rule deployment
- Building ATT&CK alerts (e.g. T1059 PowerShell)
- SOC KPIs: MTTR, MTTD, false positives, MITRE coverage
- Basic automation: Python scripts & SOAR starter playbooks

Windows & Active Directory attacks

- Introduction to Active Directory
- Kerberoasting, DCSync, Pass-the-Ticket
- Creating custom detection rules
- Analysis of malicious PowerShell scripts

Incident Response

- NIST workflow: preparation ? containment ? eradication ? recovery
- 24 h exam" simulation: time management, evidence locker, save notes
- Open-book strategies: note structure, bookmarks, checklist browser
- Post-mortem analysis & retake planning
- Post-BTL1 perspectives: BTL2, CySA+, GCIA, eJPT Blue

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.